Information Security Analyst Junior, Quality Assurance & Audit

SUMMARY

The Information Security Analyst Junior is a key member in the Quality Assurance and Audit (QAA) group of the Department of Human Services (DHS), Information Technology (IT) section. Reporting to the Quality Assurance Manager, s/he is responsible for supporting information security efforts regarding information security risk assessment and mitigation, information security policy promulgation, safeguard and compliance efforts, incident responses, and security awareness training. S/he provides authoritative advice and guidance to colleagues on any aspect of security, including training where appropriate.

The Information Security Analyst Junior must effectively ensure the that DHS systems and applications meet audit requirements for storing and processing state and federal protected data, and compliance with requirements that personal and financial data is protected against unauthorized disclosure.

PRINCIPAL DUTIES AND RESPONSIBILITIES

- Interface professionally with all levels of management, business, and technical teams.
- Conduct, review and update the annual Risk Assessment and the Security Assessment; Document and ensure communication of key risks.
- Maintain or update security standards, policies and procedures, or related documentation, and other policies as assigned.
- Identify and analyze areas of potential risk to assets, resources or success of organization. Produce reports or presentations that outline findings, explain risk positions, or recommend changes.
- Identify issues and opportunities, analyze problems and alternatives, and develop sound conclusions and recommendations.
- Analyze regulatory documentation for security requirements and analyze contracts, grants, memorandum of understanding to determine compliance with security requirements.
- Communicate security status, updates, and actual or potential problems to management.
- Review security policies, programs or procedures to ensure compliance with internal security policies, licensing requirements, or applicable government security requirements, policies and directives.
- Ensure all DHS Disaster Recovery contingency plans are reviewed and updated annually.
- Plan and contribute to development of risk management systems.
- Train users and promote security awareness to ensure systems security and to improve server and network efficiency.
- Evaluate and modify training materials to address security weaknesses and vulnerabilities.
- Review and analyze audit reports to identify risk and weaknesses in security. Gather risk-related data from internal or external resources.
- Provide leadership to identify process improvements and participate in their implementation to promote continuous improvement.

EDUCATION / EXPERIENCE
A bachelor's degree in Information Technology, Information Management Systems, Computer Science, and/or related technical degrees or coursework from an accredited college or university.

A minimum of one (1) year of increasingly responsible IT experience in one or a combination of the following: 1) information security program design and implementation, or 2) information security risk analysis and mitigation, or 3) information security policy, standards and procedures creation and implementation.

An equivalent combination of education and/or experience may be acceptable.

Certified Information Security Systems Professional (CISSP) is a plus.

SKILLS
This position requires:

- Dedication and commitment to customer service focused delivery of solutions
- Ability to build trust and teamwork in difficult situations across all departmental boundaries
- Excellent organizational and planning skills
- Exceptional verbal and written communication skills, with the soft skills necessary to hold meaningful and effective communications with business and technical staff
- Ability to lead programs for improving the security within an organization or project, including identification and management of critical success factors
- Ability to create, maintain, and review documentation of all types, including audit documentation, security standards, and quality management plans
- Ability to identify current or future problems or opportunities, analyze, synthesize, and compare information to understand issues and cause/effect relationships, and explore alternative solutions to support sound decision making.
- Knowledge of Security Best Practices, Policy and Standards, and Regulatory and Statutory Requirements
- Demonstrated ability to display and promote high standards of ethical conduct and behaviors consistent with departmental and government standards
- Ability to resolve or escalate issues in a timely manner
- Ability to approach others in a professional tactful manner, react well under pressure, accept responsibility for own actions and follow through on commitments
- Ability to deal with frequent change, delays, or unexpected events and to quickly and easily adapt to changing priorities
- Intermediate level skills using Microsoft Office software, including Word, PowerPoint, Excel, and Visio

The State of TN is an Equal Opportunity Employer.